

Amendments to the Claims

1-3. (Canceled)

4. (Currently amended) A method of recording contents information, comprising the steps of:

generating a signal representative of a key from authenticator-value information and key base information, the authenticator-value information representing a specified authenticator value, the key base information containing identification information which is set to reproduce the specified authenticator value according to a predetermined degeneration function;

encrypting at least the identification information in the key base information to convert the key base information into encryption-resultant key base information;

encrypting contents information into encryption-resultant contents information in response to the key signal; and

recording the encryption-resultant key base information and the encryption-resultant contents information ;

wherein the identification information in the key base information contains at least one of 1) information about a region or regions corresponding to one or more countries, one or more zones, or one or more spaces, 2) information about identification of an individual, 3) information about identification of a group of persons, 4) information about a rating, 5) information about identification of an apparatus maker or a device maker, 6) information about identification of a contents provider, 7) information about time, 8) information about contents authors, 9) information about identification of a reproducing apparatus or a reproducing device, 10) information about identification of a connection apparatus or a connection device, 11) information about identification of a medium on which contents information is recorded, 12) information about identification of contents information, and 13) information about accounting.

5-6. (Canceled)

7. (Original) A transmission medium for transmitting encryption-resultant key base information and encryption-resultant contents information, wherein the encryption-resultant key base information and the encryption-resultant contents information are generated by the steps of generating a signal representative of a key from authenticator-value information and key base information, the authenticator-value information representing a specified authenticator value, the key base information containing identification information which is set to reproduce the specified authenticator value according to a predetermined degeneration function; encrypting at least the identification information in the key base information to convert the key base information into encryption-resultant key base information; and encrypting contents information into encryption-resultant contents information in response to the key signal.

8. (Original) A recording medium loaded with encryption-resultant key base information and encryption-resultant contents information, wherein the encryption-resultant key base information and the encryption-resultant contents information are generated by the steps of generating a signal representative of a key from authenticator-value information and key base information, the authenticator-value information representing a specified authenticator value, the key base information containing identification information which is set to reproduce the specified authenticator value according to a predetermined degeneration function; encrypting at least the identification information in the key base information to convert the key base information into encryption-resultant key base information; and encrypting contents information into encryption-resultant contents information in response to the key signal.

9. (Currently amended) A method ~~as recited in claim 3, of transmitting contents information, comprising the steps of:~~

~~generating a signal representative of a key from authenticator-value information and key base information, the authenticator-value information representing a specified~~

authenticator value, the key base information containing identification information which is set to reproduce the specified authenticator value according to a predetermined degeneration function:

encrypting at least the identification information in the key base information to convert the key base information into encryption-resultant key base information;

encrypting contents information into encryption-resultant contents information in response to the key signal; and

transmitting the encryption-resultant key base information and the encryption-resultant contents information;

wherein the identification information in the key base information contains at least one of 1) information about a region or regions corresponding to one or more countries, one or more zones, or one or more spaces, 2) information about identification of an individual, 3) information about identification of a group of persons, 4) information about a rating, 5) information about identification of an apparatus maker or a device maker, 6) information about identification of a contents provider, 7) information about time, 8) information about contents authors, 9) information about identification of a reproducing apparatus or a reproducing device, 10) information about identification of a connection apparatus or a connection device, 11) information about identification of a medium on which contents information is recorded, 12) information about identification of contents information, and 13) information about accounting.

10-12. (Canceled)

13. (Currently amended) A method of recording contents information, comprising the steps of:

generating a signal representative of a key from key base information containing identification information which is set to reproduce a specified authenticator value according to a predetermined degeneration function;

encrypting at least the identification information in the key base information to convert the key base information into encryption-resultant key base information;

encrypting contents information into encryption-resultant contents information in response to the key signal; and

recording the encryption-resultant key base information and the encryption-resultant contents information:-

wherein the identification information in the key base information contains at least one of 1) information about a region or regions corresponding to one or more countries, one or more zones, or one or more spaces, 2) information about identification of an individual, 3) information about identification of a group of persons, 4) information about a rating, 5) information about identification of an apparatus maker or a device maker, 6) information about identification of a contents provider, 7) information about time, 8) information about contents authors, 9) information about identification of a reproducing apparatus or a reproducing device, 10) information about identification of a connection apparatus or a connection device, 11) information about identification of a medium on which contents information is recorded, 12) information about identification of contents information, and 13) information about accounting.

14. (Currently amended) An apparatus for transmitting contents information, comprising:

means for generating a signal representative of a key from key base information containing identification information which is set to reproduce a specified authenticator value according to a predetermined degeneration function;

means for encrypting at least the identification information in the key base information to convert the key base information into encryption-resultant key base information;

means for encrypting contents information into encryption-resultant contents information in response to the key signal; and

means for transmitting the encryption-resultant key base information and the encryption-resultant contents information:-

wherein the identification information in the key base information contains at least one of 1) information about a region or regions corresponding to one or more

countries, one or more zones, or one or more spaces, 2) information about identification of an individual, 3) information about identification of a group of persons, 4) information about a rating, 5) information about identification of an apparatus maker or a device maker, 6) information about identification of a contents provider, 7) information about time, 8) information about contents authors, 9) information about identification of a reproducing apparatus or a reproducing device, 10) information about identification of a connection apparatus or a connection device, 11) information about identification of a medium on which contents information is recorded, 12) information about identification of contents information, and 13) information about accounting.

15. (Currently amended) An apparatus for recording contents information, comprising:

means for generating a signal representative of a key from key base information containing identification information which is set to reproduce a specified authenticator value according to a predetermined degeneration function;

means for encrypting at least the identification information in the key base information to convert the key base information into encryption-resultant key base information;

means for encrypting contents information into encryption-resultant contents information in response to the key signal; and

means for recording the encryption-resultant key base information and the encryption-resultant contents information:;

wherein the identification information in the key base information contains at least one of 1) information about a region or regions corresponding to one or more countries, one or more zones, or one or more spaces, 2) information about identification of an individual, 3) information about identification of a group of persons, 4) information about a rating, 5) information about identification of an apparatus maker or a device maker, 6) information about identification of a contents provider, 7) information about time, 8) information about contents authors, 9) information about identification of a reproducing apparatus or a reproducing device, 10) information about identification of a

connection apparatus or a connection device, 11) information about identification of a medium on which contents information is recorded, 12) information about identification of contents information, and 13) information about accounting.

16. (Original) A transmission medium for transmitting encryption-resultant key base information and encryption-resultant contents information, wherein the encryption-resultant key base information and the encryption-resultant contents information are generated by the steps of generating a signal representative of a key from key base information containing identification information which is set to reproduce a specified authenticator value according to a predetermined degeneration function; encrypting at least the identification information in the key base information to convert the key base information into encryption-resultant key base information; and encrypting contents information into encryption-resultant contents information in response to the key signal.

17. (Original) A recording medium loaded with encryption-resultant key base information and encryption-resultant contents information, wherein the encryption-resultant key base information and the encryption-resultant contents information are generated by the steps of generating a signal representative of a key from key base information containing identification information which is set to reproduce a specified authenticator value according to a predetermined degeneration function; encrypting at least the identification information in the key base information to convert the key base information into encryption-resultant key base information; and encrypting contents information into encryption-resultant contents information in response to the key signal.

18. (Currently amended) A method ~~as recited in claim 12, of transmitting contents information, comprising the steps of:~~

generating a signal representative of a key from key base information containing identification information which is set to reproduce a specified authenticator value according to a predetermined degeneration function;

encrypting at least the identification information in the key base information to convert the key base information into encryption-resultant key base information;
encrypting contents information into encryption-resultant contents information in response to the key signal; and
transmitting the encryption-resultant key base information and the encryption-resultant contents information;

wherein the identification information in the key base information contains at least one of 1) information about a region or regions corresponding to one or more countries, one or more zones, or one or more spaces, 2) information about identification of an individual, 3) information about identification of a group of persons, 4) information about a rating, 5) information about identification of an apparatus maker or a device maker, 6) information about identification of a contents provider, 7) information about time, 8) information about contents authors, 9) information about identification of a reproducing apparatus or a reproducing device, 10) information about identification of a connection apparatus or a connection device, 11) information about identification of a medium on which contents information is recorded, 12) information about identification of contents information, and 13) information about accounting.

19. (Original) A method of decrypting encryption-resultant contents information generated by an encrypting side which implements the steps of generating a signal representative of a key from authenticator-value information and key base information, the authenticator-value information representing a specified authenticator value, the key base information containing identification information which is set to reproduce the specified authenticator value according to a predetermined degeneration function; and encrypting contents information into encryption-resultant contents information in response to the key signal; the method comprising the steps of:

reproducing the authenticator-value information representative of the specified authenticator value from the identification information in the key base information according to the predetermined degeneration function;

reproducing the key signal from the reproduced authenticator-value information and the key base information; and

decrypting the encryption-resultant contents information into the original contents information in response to the reproduced key signal.

20. (Original) A method of decrypting encryption-resultant contents information generated by an encrypting side which implements the steps of generating a signal representative of a key from authenticator-value information and key base information, the authenticator-value information representing a specified authenticator value, the key base information containing identification information which is set to reproduce the specified authenticator value according to a predetermined degeneration function; encrypting at least the identification information in the key base information to convert the key base information into encryption-resultant key base information; and encrypting contents information into encryption-resultant contents information in response to the key signal; the method comprising the steps of:

decrypting the encryption-resultant key base information into the original key base information;

reproducing the authenticator-value information representative of the specified authenticator value from the identification information in the original key base information according to the predetermined degeneration function;

reproducing the key signal from the reproduced authenticator-value information and the original key base information; and

decrypting the encryption-resultant contents information into the original contents information in response to the reproduced key signal.

21. (Original) An apparatus for decrypting encryption-resultant contents information generated by an encrypting side which implements the steps of generating a signal representative of a key from authenticator-value information and key base information, the authenticator-value information representing a specified authenticator value, the key base information containing identification information which is set to reproduce the

specified authenticator value according to a predetermined degeneration function; encrypting at least the identification information in the key base information to convert the key base information into encryption-resultant key base information; and encrypting contents information into encryption-resultant contents information in response to the key signal; the apparatus comprising:

means for decrypting the encryption-resultant key base information into the original key base information;

means for reproducing the authenticator-value information representative of the specified authenticator value from the identification information in the original key base information according to the predetermined degeneration function;

means for reproducing the key signal from the reproduced authenticator-value information and the original key base information; and

means for decrypting the encryption-resultant contents information into the original contents information in response to the reproduced key signal.

22. (Original) A method of decrypting encryption-resultant contents information generated by an encrypting side which implements the steps of generating a signal representative of a key from key base information containing identification information which is set to reproduce a specified authenticator value according to a predetermined degeneration function; and encrypting contents information into encryption-resultant contents information in response to the key signal; the method comprising the steps of:

reproducing the authenticator-value information representative of the specified authenticator value from the identification information in the key base information according to the predetermined degeneration function;

reproducing the key signal from the key base information;

deciding whether or not the reproduced authenticator-value information is correct;

decrypting the encryption-resultant contents information in response to the reproduced key signal when it is decided that the reproduced authenticator-value information is correct; and

altering the reproduced key signal into a wrong key signal and decrypting the encryption-resultant contents information in response to the wrong key signal when it is decided that the reproduced authenticator-value information is not correct.

23. (Original) A method of decrypting encryption-resultant contents information generated by an encrypting side which implements the steps of generating a signal representative of a key from key base information containing identification information which is set to reproduce a specified authenticator value according to a predetermined degeneration function; encrypting at least the identification information in the key base information to convert the key base information into encryption-resultant key base information; and encrypting contents information into encryption-resultant contents information in response to the key signal; the method comprising the steps of:

decrypting the encryption-resultant key base information into the original key base information;

reproducing the authenticator-value information representative of the specified authenticator value from the identification information in the original key base information according to the predetermined degeneration function;

reproducing the key signal from the original key base information;

deciding whether or not the reproduced authenticator-value information is correct;

decrypting the encryption-resultant contents information in response to the reproduced key signal when it is decided that the reproduced authenticator-value information is correct; and

altering the reproduced key signal into a wrong key signal and decrypting the encryption-resultant contents information in response to the wrong key signal when it is decided that the reproduced authenticator-value information is not correct.

24. (Original) An apparatus for decrypting encryption-resultant contents information generated by an encrypting side which implements the steps of generating a signal representative of a key from key base information containing identification information

which is set to reproduce a specified authenticator value according to a predetermined degeneration function; encrypting at least the identification information in the key base information to convert the key base information into encryption-resultant key base information; and encrypting contents information into encryption-resultant contents information in response to the key signal; the apparatus comprising:

means for decrypting the encryption-resultant key base information into the original key base information;

means for reproducing the authenticator-value information representative of the specified authenticator value from the identification information in the original key base information according to the predetermined degeneration function;

means for reproducing the key signal from the original key base information;

means for deciding whether or not the reproduced authenticator-value information is correct;

means for decrypting the encryption-resultant contents information in response to the reproduced key signal when it is decided that the reproduced authenticator-value information is correct; and

means for altering the reproduced key signal into a wrong key signal and decrypting the encryption-resultant contents information in response to the wrong key signal when it is decided that the reproduced authenticator-value information is not correct.

25. (Original) A method of decrypting encryption-resultant contents information generated by an encrypting side which implements the steps of generating a signal representative of a key from key base information containing identification information which is set to reproduce a specified authenticator value according to a predetermined degeneration function; and encrypting contents information into encryption-resultant contents information in response to the key signal; the method comprising the steps of:

reproducing the authenticator-value information representative of the specified authenticator value from the identification information in the key base information according to the predetermined degeneration function;

reproducing the key signal from the key base information;

deciding whether or not the reproduced authenticator-value information is correct;

decrypting the encryption-resultant contents information in response to the reproduced key signal when it is decided that the reproduced authenticator-value information is correct; and

failing to decrypt the encryption-resultant contents information in response to the reproduced key signal when it is decided that the reproduced authenticator-value information is not correct.

26. (Original) A method of decrypting encryption-resultant contents information generated by an encrypting side which implements the steps of generating a signal representative of a key from key base information containing identification information which is set to reproduce a specified authenticator value according to a predetermined degeneration function; encrypting at least the identification information in the key base information to convert the key base information into encryption-resultant key base information; and encrypting contents information into encryption-resultant contents information in response to the key signal; the method comprising the steps of:

decrypting the encryption-resultant key base information into the original key base information;

reproducing the authenticator-value information representative of the specified authenticator value from the identification information in the original key base information according to the predetermined degeneration function;

reproducing the key signal from the original key base information;

deciding whether or not the reproduced authenticator-value information is correct;

decrypting the encryption-resultant contents information in response to the reproduced key signal when it is decided that the reproduced authenticator-value information is correct; and

failing to decrypt the encryption-resultant contents information in response to the reproduced key signal when it is decided that the reproduced authenticator-value information is not correct.

27. (Original) An apparatus for decrypting encryption-resultant contents information generated by an encrypting side which implements the steps of generating a signal representative of a key from key base information containing identification information which is set to reproduce a specified authenticator value according to a predetermined degeneration function; encrypting at least the identification information in the key base information to convert the key base information into encryption-resultant key base information; and encrypting contents information into encryption-resultant contents information in response to the key signal; the apparatus comprising:

means for decrypting the encryption-resultant key base information into the original key base information;

means for reproducing the authenticator-value information representative of the specified authenticator value from the identification information in the original key base information according to the predetermined degeneration function;

means for reproducing the key signal from the original key base information;

means for deciding whether or not the reproduced authenticator-value information is correct;

means for decrypting the encryption-resultant contents information in response to the reproduced key signal when it is decided that the reproduced authenticator-value information is correct; and

means for failing to decrypt the encryption-resultant contents information in response to the reproduced key signal when it is decided that the reproduced authenticator-value information is not correct.

28. (Original) A method as recited in claim 19, wherein the identification information in the key base information contains at least one of 1) information about a region or regions corresponding to one or more countries, one or more zones, or one or more

spaces, 2) information about identification of an individual, 3) information about identification of a group of persons, 4) information about a rating, 5) information about identification of an apparatus maker or a device maker, 6) information about identification of a contents provider, 7) information about time, 8) information about contents authors, 9) information about identification of a reproducing apparatus or a reproducing device, 10) information about identification of a connection apparatus or a connection device, 11) information about identification of a medium on which contents information is recorded, 12) information about identification of contents information, and 13) information about accounting.